Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

QaASs: QoS aware adaptive security scheme for video streaming in MANETs

Tahsin Arafat Reza[*], *Michel Barbeau*

School of Computer Science, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada

Keywords:
Ad hoc network
QoS
Multimedia security
Video encryption
Adaptive security
Elliptic curve cryptography

A B S T R A C T

Real-time video streaming is delay sensitive. It has minimum bandwidth and QoS requirements. Achieving target QoS for video streaming is challenging in a decentralized and self-organized MANET. Cryptography algorithms offer confidentiality of shared data, but they have computation cost. Our work addresses the issue of delay overhead caused by the introduction of cryptography that directly affects video streaming performance. Our proposal is motivated by the possibilities of adaptive security and multimedia service. We make an effort to identify why, when and how to deploy adaptation. We propose QaASs (QoS aware Adaptive Security scheme), an adaptive mechanism that counters the effect of delay overhead by adapting cryptography and multimedia properties, providing QoS while maintaining a required level of security. We evaluate our proposal through implementation and simulation.

1. Introduction

A Mobile Ad hoc Network (MANET) is a communications network where there is no fixed infrastructure or central authority. The nodes are self-organized and communicate with each other directly or through intermediate nodes. Nodes act as hosts and routers. No static topology is guaranteed. There is a growing interest for real-time video streaming in MANETs. Possible usages are remote surveillance, environmental or wildlife monitoring, rescue operations, telemedicine in adverse environments, collaborative unmanned remote exploration, ad hoc network of UAVs (Unmanned Arial Vehicles) and UWVs (Unmanned Under Water Vehicles). In a VANET (Vehicular Ad hoc Network), peers can engage in video conference as well as stream media in an ad hoc manner.

In a computer network, security measures are deployed as a protection against malicious attacks or intentional faults that disrupt regular operations and unauthorized access to resources and information. The physical construction and functional characteristics of a MANET make it vulnerable and susceptible to malicious attacks. Absence of infrastructure, broadcast nature of wireless transmission, sole dependency on wireless links, dynamic topology, and multihop routing have been identified as the primary features that make MANETs vulnerable to malicious attacks (Djenouri et al., 2005). Security techniques for infrastructure-based networks are often not applicable to MANETs. For example, the use of a unique certification authority (CA) is against the core concept of infrastructure-less networks. *Eavesdropping*, *Tunneling*, *Spoofing*, *Rushing*, *Wormholes*, *Black holes* and various DoS (Denial of Service) attacks (Djenouri et al., 2005) are examples of security setbacks in MANETs. *Confidentiality* is a must have requirement for distributing and sharing sensitive information (Stallings, 2011). Confidentiality refers to the protection against unauthorized disclosure of information. Cryptography provides security for digital contents. Real-time video streaming is delay sensitive, involves encoding and decoding and has minimum bandwidth and other QoS (Quality of Service) requirements (Perkins and Hughes, 2002). QoS is a set of service requirements (e.g., delay, data rate and error

[*] *Corresponding author*. Tel.: +1 6473385284.
E-mail addresses: treza@connect.carleton.ca (T.A. Reza), barbeau@scs.carleton.ca (M. Barbeau).

2214-2126/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jisa.2013.08.003

correction) to be met by the network while transporting a packet data stream. Achieving target QoS for video streaming is challenging in an unpredictable MANET. Cryptography algorithms could be computationally intensive. Computation overhead introduced by cryptography operations may cause additional delay to video streaming that could directly influence playback experience.

Our work addresses the issue of high delays caused by the introduction of cryptography that directly affects video streaming performance. A MANET can be composed of a diverse range of devices with different computation capabilities. The performance of a computationally intensive cryptography process varies depending on the available system resource (e.g., physical memory and number of running threads). A cryptography process may introduce additional, yet unavoidable delay overhead. If a traffic source knows the capability of a target device, e.g., the throughput of a cryptography process, then it can infer appropriate cryptography parameters that avoid a performance bottleneck. Furthermore, it is possible to control multimedia traffic, thus the amount of data to be processed by a cryptography processor. Traffic load influences network latency as well as congestion, thus packet delivery ratio. By adjusting multimedia parameters, it is possible to control the overall delay as well as provide QoS. The receiver of multimedia data can provide periodic feedback to the source with information such as transmission delay, delay jitter, effective frame rate and frame loss ratio. Hence, an adaptive mechanism that trades off between security and QoS parameters is a feasible solution to the addressed problem.

We propose QaASs (QoS aware Adaptive Security scheme), a runtime adaptive mechanism that counters the high delay adapting cryptography and multimedia properties, providing QoS while maintaining a required level of security. The mechanism is designed around a cryptography delay threshold value and considers cryptography process throughput and delay, and video reception rate. QaASs defines *why*, *when* and *how* to deploy adaptation. We demonstrate the effectiveness of our proposal in a number of scenarios demanding different requirements. Results are confirmed with a 95% confidence level (Devore, 2011).

The rest of the paper is organized in four sections. In Section 2, we present a literature review related to the problem of interest. Relevant background information are detailed in Section 3. We present a series of evaluations in Section 4 to demonstrate how cryptography influences video streaming. In Section 5, we describe our proposal. Simulation and results are documented in Section 6. Section 7 concludes the paper and outlines future work.

2. Related work

The notion of adaptive security takes root in autonomic security management (He et al., 2011). Shnitko (Shnitko, 2003) identified adaptive security as a problem of optimal control of an object whose state is influenced by a set of adaptable factors and environment parameters. He stressed on the necessity of adaptive approaches for information security in order to cope with the uncertainty of the environment. A class of adaptive security approaches focus on defying the impact of performance degradation and resource exhaustion as a result of security provisioning. Venkatramani et al. (2003), Pereira and Tarouco (2009), Ben Mahmoud et al. (2010) and Alia et al. (2010) used adaptive security for multimedia QoS, Younis et al. (2009), Taddeo et al. (2009), He et al. (2011) and Oliveira et al. (2011) for energy efficiency, and Alia et al. (2010) and Samad and Makram (2010) for computing resource efficiency. Nijim and Ali (Nijim and Ali, 2008) proposed an adaptive security approach to enhance disk response time. Son et al. (1996) proposed an adaptive security method for time-critical DBMSs (Database Management System) by partially compromising security for improved timeliness. Preda et al. (Preda et al., 2011) described an adaptation technique for policy deployment and dynamic refinement of contextual security policies where security devices are unaware of context semantics. Zou et al. (Zou et al., 2002) proposed the use of adaptive security to create an intelligent firewall to trade off between security and performance. Ben Mahmoud et al., (2010) and Taddeo et al., (2009) used AHP (Analytical Hierarchical Process) for modeling an adaptive security solution. Zou et al., (2002) and Alampalayam and Kumar (2003) used a fuzzy logic-based approach. Alia et al. (Alia et al., 2010) presented a Component Composition Selection problem based adaptation model enabling fine-grained trade-offs between QoS and security. He et al. (He et al., 2011) presented a DSL (Domain Specific Language) (Van Deursen et al., 2000) to describe security adaptation policies for self-protection with emphasizes on runtime adaptation.

Cryptography can be applied to real-time streaming video in several manners. Encryption can be employed in the transform domain, within the video encoder. For example, in Gibson et al. (2004) and Meyer and Gadegast (2000) the DC components and motion vectors are encrypted. Format compliance is a key issue for this approach. The second approach is post compression encryption, where encoded video frames are encrypted individually. The third approach is encrypting the packet payload of the multimedia streaming protocol, e.g., RTP (Perkins, 2003). Spanos and Maples (Spanos and Maples, 1995) were among the first to introduce selective encryption by encrypting only the I-frames of MPEG coded video. Kamphenkel and Blank (Kamphenkel et al., 2008) proposed an adaptive security model called Intelligent Network (IN) to address the issue of delay overhead caused by cryptography. IN offers security and congestion aware path selection and allows separate streams in different classes of reliability. Vaidya et al. (Vaidya et al., 2009) proposed a secured multipath traffic allocation technique for VoIP in MANETs. The core bitstream of G.727 (ITU-T, 1990) coded data is transmitted over the primary path (fail-safe and higher data rate) and the enhancement bitstream over the secondary path. In a similar work, Gibson et al. (Gibson et al., 2004) proposed selective encryption for scalable speech coding (SNR) (Dong et al., 2002) over MANETs. SECMPEG (Meyer and Gadegast, 2000), proposed by Meyer and Gadegast, selectively encrypts DC components, I-blocks and motion vectors, sequence and slice headers of MPEG video according to the security level. Tang incorporated cryptography at the video coding level to achieve compression and encryption in one step (Tang, 1996). Tang's work was among the firsts that